



**STRATEGY
RESEARCH
PROJECT**

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

**STRATEGIC EFFECTS OF THE ARMY ENTERPRISE
MANAGEMENT TRANSFORMATION**

BY

MR. DONAL E. MEYNIG
Department of the Army Civilian

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited

USAWC CLASS OF 2002



U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

20020806 317

USAWC STRATEGY RESEARCH PROJECT

STRATEGIC EFFECTS OF THE ARMY ENTERPRISE MANAGEMENT TRANSFORMATION

by

Mr. Donal E. Meynig
Department of the Army Civilian

Professor Kevin Cogan
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

ABSTRACT

AUTHOR: Mr. Donal E. Meynig

TITLE: The Strategic Effects of the Army Enterprise Management Transformation

FORMAT: Strategy Research Project

DATE: 09 April 2002

PAGES: 29

CLASSIFICATION: Unclassified

The Army is in the early stages of a significant Information Technology (IT) transformation that will have far reaching effects on current and future IT policy and operations Army wide. This research project will look at the implications of this transformation and develop pro and con strategic effects. Feedback will be gathered from Army echelons that will be affected by the transformation. Historical research will address the Army's previous attempt to make a similar transition and what might be gained in retrospect from that experience.

TABLE OF CONTENTS

ABSTRACT	iii
PREFACE	vii
STRATEGIC EFFECTS OF THE ARMY ENTERPRISE MANAGEMENT TRANSFORMATION	1
EVENTS LEADING TO THE PRESENT	1
INFORMATION SYSTEMS COMMAND (ISC)	2
IVORY TOWER	2
INSTALLATIONS SOLVING THEIR OWN PROBLEMS	2
NO STANDARDIZATION	3
ISC REORGANIZATION	3
ARMY TRANSFORMATION	4
THE NEW ADMINISTRATION	5
QUADRENNIAL DEFENSE REVIEW (QDR)	6
SEPTEMBER 11, 2001	8
THE PLAN	8
ARMY KNOWLEDGE MANAGEMENT (AKM)	10
THE EFFECT	11
THE OBJECTION	12
THE FUTURE	13
CONCLUSION	14
ENDNOTES	17
BIBLIOGRAPHY	21

PREFACE

For many years there has existed a need for consolidation and standardization of Army IT resources. What has not been present is any widespread, unified approach by senior Army leadership to strongly support the concentrated effort necessary to bring about a dynamic and lasting change. There is significant evidence to indicate that a change in direction and policy may now be possible. The Chief of Staff of the Army, GEN Eric Shinseki, began transforming the Army three years ago. In that transformation is the recognition that IT is a critically key element affecting every other factor in the transformation plan. The Air Force began making similar changes in 2001 when they began linking all IT into a common web portal. Also in 2001 the Navy saw similar strategies and began standardizing and consolidating all land based IT. A new administration was elected and took office in that same year. The appointed senior Department of Defense leaders, to include the Service Secretaries, have much in common in their backgrounds, mainly, successful senior executive experience in the corporate world, extensive senior military background and significant experience in bringing about change in their previous organizations. The tragedies of September 11, 2001 also brought reinforcement for the transformation and in particular, the importance of IT and communications as critical players in Homeland Defense. All the ingredients for successful transformation seem to be in place. The question is will they be powerful enough to affect dramatic and lasting change? The time is right, the players are right and the ingredients are right to make this transformation a lasting reality.

STRATEGIC EFFECTS OF THE ARMY ENTERPRISE MANAGEMENT TRANSFORMATION

The most important transformation that we are facing is the transformation from the Industrial to the Information Age. To the extent we do that well, all of our other efforts in transformation will prosper. To the extent that we don't, all of those efforts will be for naught.

—ADM (RET) Arthur Cebrowski

Significant lasting change in a large public organization is always difficult and usually impossible to complete unless there is a unified buy-in among the most senior level executives who have the conviction and authority to act on their beliefs. Even when you have those conditions there must also be widespread support from the funding sector, in this case the voting public, to understand and accept the need for the change.

The events of 11 September 2001 are reshaping the public thinking about the strategic direction U.S. military operations should be headed in this country and around the world. The fast changing world of Information Technology (IT) is now moving even faster, especially in the U.S. Army. As we will see, a major transformation was already in progress in the U.S. Army before the recent tragedy. The current situation only reinforces the need for such changes and validates the speed and attention being placed on implementation.

This report begins with a macro review of the history of several previous IT reorganization and transformation attempts. This will establish the background necessary to understand the biases that affect current thinking about future changes. Next the report examines the highlights of the current IT transformation and discusses the immediate actions that are being taken to implement this guidance in the U.S. Army and the strategic effects that can be expected. It will also look at possible objections to the transformation and the reasons for those objections. Finally it will briefly touch on the future of IT in the Army.

EVENTS LEADING TO THE PRESENT

The history of automation in the Army has progressed from the development of the very first large-scale mainframe computer in the world, the ENIAC, to a broad based desktop environment not unlike those in place in the corporate structure the world over. The computer usage pendulum swings from strictly tactical use in the beginning to administrative, to command and control, to today where every facet of the military is dependent on IT for mission success. A detailed chronology of every IT event that has taken place in the Army over the past fifty-five

years is not relevant for this paper. The highlights that have brought us to our present way of thinking about and using IT are.

INFORMATION SYSTEMS COMMAND (ISC)

ISC was the first significant organization to influence current IT thinking and philosophy. Starting in the 1980's, the structure was an Army Command level organization with directly reporting cells located at every Army installation. IT support was provided locally by the on site ISC organization that had its own separate funding and chain-of-command, which did not include the installation commander.¹ Services provided were not always timely and the priorities were not always in concert with what the commander thought was most important for his organization. Equipment was often unreliable but that was the state of the computer industry in the late 1970's. The regional approach tried to solve the problems identified by the largest number of installations. These turned into big projects requiring years to complete taking people and money away from immediate local problems. Commanders were not happy.²

IVORY TOWER

At the local level, ISC organizations became complacent, often losing touch with the realities of the installation needs. The installation commander had little or no authority over the ISC organization. The technical ISC staff did not understand the functional needs being requested by the organizations and often turned down requests for service. IT funding in the ISC chain-of-command was often held at the command level to pay for multi-installation programs being developed. Most of the funding that reached the local level was used for mainframe computer replacement and maintenance leaving very little discretionary funding for the ISC organization to support local unique requirements. The result was that ISC organizations were viewed as being out of touch and not responsive to user requirements, creating an ivory tower image that lead installation commanders to search for new ways to meet their IT needs.³

INSTALLATIONS SOLVING THEIR OWN PROBLEMS

The Personal Computer (PC) made its debut into the Army in an informal way in the 1980's. The IT technical community viewed it as a toy not capable of any significant processing ability. They ignored it. Functional users saw it as a way to meet their immediate needs which were not being satisfied by the on site ISC organizations. They found that members of their functional staffs had PC's at home and could write simple programs to solve simple needs. Commanders bought PC's and began solving their own problems. As the PC grew in power,

storage capacity, and capability, larger applications were written. Local Area Networks connected the PC's together and formed processing centers that would rival some ISC computer centers. Under functional user control, these systems solved an immediate local problem but usually were not compatible with similar systems at other installations. Quite often these systems were subsets or duplications of higher-level systems written in whatever programming language the programmer liked and knew how to use.⁴

NO STANDARDIZATION

With no central organization watching or approving new systems and hardware, incompatibility became the standard. The Army amassed a conglomeration of hardware that didn't communicate with other hardware, programming languages that would not talk to each other, no documentation for written programs, and untrained users and systems operators. When the person that wrote a program left the organization, quite often the program had to be scrapped the first time it malfunctioned because no one knew how to fix it. The writers had not taken the time to document their programs.

No policy existed that established who had the authority to acquire PC's or software. As PC's became very powerful, they grew into servers with no authorization documents establishing control and responsibility for their use. More sophisticated systems were developed which only compounded the problem. Support staffs to run non-standard systems emerged, reallocated from the existing functional staff positions. Servers were linked. Functional systems grew even larger, amazingly with no compatibility or standards checks and no formal approval process. The point at which a local organization wanted to expand usage of their system to another installation is where the problems began. Standards, hardware and software compatibility, and connectivity methods required interface with the IT organizations in order to make the connection. Quite often the two systems could not connect because functional developers did not know about or use any programming standards during development. Conflicts were constant as organizations continued to solve their own problems in a vacuum, oblivious to the surrounding duplications and incompatibilities. Significant dollars were wasted during this period buying the wrong or incompatible equipment.⁵

ISC REORGANIZATION

In the 1990's the ISC reassigned the on site DOIM's back to the installation commanders where they became a part of the local organization.⁶ These cells had to assume responsibility for standardizing the functional systems and incorporating them into their current operating environment where possible. Many were not salvageable because there was no documentation

or the software used was incompatible with existing standard software. These systems had to either be scrapped or re-written causing further discord between the customers and the IT staff. The level of discontent increased or decreased over time depending on the installation and the technical expertise and customer skills of all parties involved. In many cases the functional developers were reassigned to the DOIM staff with mixed emotions on both sides about the wisdom of that decision. Some felt abandoned by their proponent organizations. Others saw an opportunity rise to positions of leadership in those organizations and attempt to change the nature of the way business was conducted. Some users continued to run their own systems electing to fund and staff them out of their own resources often with the blessing of the commander.⁷

The lasting effect of these turbulent IT transitions back and forth was a lack of understanding of the workings of IT by the command structure and a general feeling of mistrust on the part of commanders about the allegiance and alignment of their new IT staff and reinforcement of the concept that believes you get more things done your way when you are in direct control of the people and the money.

ARMY TRANSFORMATION

GEN Shinseki began the Army transformation as he assumed his duties as Army Chief of Staff in 1998 and called attention to the changing world around us. He started the Army in a new direction calling for radical changes in the way we fight and the weapons we fight with. He also defined the new types of enemies we will face in the coming century. Most importantly, GEN Shinseki outlined the critical need to transform the Army into a network-centric, knowledge-based force in order to improve decision dominance of the war fighters and business stewards in the battle space, in our organizations, and in our mission practices. Joint communications and systems to accomplish those tasks will be a key ingredient to success. In the early portion of his tour, GEN Shinseki did not seem to enjoy overwhelming support for what he was trying to accomplish from either inside or outside the Army. Army senior leadership seemed poised in the tradition of hanging on to their last successful war and looking with some skepticism on the massive transformation being proposed. The American public did not really care, as long as it didn't cost any more and perhaps less than current defense spending.⁸

Some success was generated and a gradual trend toward general acceptance of the changes began. Other military services also suggested similar changes that caused the momentum to increase at a higher rate than had been experienced in many years. But even that increase was not nearly enough to convince senior leaders that something significant

and long lasting was evolving. That would not happen until a much larger group of key individuals began accepting the tenets of transformation.⁹ What was building from within the services was a good start but it did not look any different than many other change attempts everyone had experienced over the course of their careers. What would help GEN Shinseki and the other service chiefs to make the transformation move faster would be reinforcement in the form of power and influence to validate just how big the changes would be and how serious their superiors were about supporting those changes.

THE NEW ADMINISTRATION

The inauguration of president Bush in 2001 brought in a new cabinet and the appointment of fresh senior leadership for the Department of Defense (DOD). Unique to the transformation was the careful selection of a Secretary of Defense, Deputy Secretary of Defense, and Secretaries of the Army, Navy and Air Force all with significant experience in both the corporate world and the military environment. Each brought to the Department of Defense an extraordinary wealth of knowledge about the defense industry, the Defense Department, and about private business and what it takes to bring about fundamental change in a large complicated organization.¹⁰ The President picked his leaders with what appears to be specific objectives in mind. Having been the Secretary of Defense in a previous administration, then engineering a successful turnaround as Chief Executive Officer (CEO) of a worldwide pharmaceutical company, Mr. Rumsfeld was well aware of the daunting task he faced.¹¹ Over the years he had seen various attempts to change one branch of the military or another. He observed attempts by other Secretaries of Defense to change DOD with little success.

If an organization of this size is going to make a successful massive transformation, it must be well coordinated. All key players must support the change and understand the need to compromise for the overall good of the larger group. To do that one must build a solid team of like-minded key leaders who are dynamic thinkers with proven track records for quick, effective and cooperative action. They must all support the application of corporate "bottom line" to the equation to gain efficiencies in light of shrinking budgets. The concept of performance based programs, manpower, offices, and overhead give a new perspective to the decision-making process, especially if all key players think, act and execute together in this manner. That winning combination could transform the military services and DOD simultaneously.¹²

Picking this particular group of individuals with common backgrounds for the Secretary of Defense and the military service chiefs filled the bill for creating success. Keeping a team such as this together long enough to initiate and sustain real change becomes the real problem. No

one knows exactly how long the team will remain together. All sorts of outside factors can affect the length of time any one or all of these players will spend in their positions. Resignation of high ranking officials can happen at anytime for a variety of reasons. Should that happen, who knows how that might affect the balance of that team or what the team might accomplish? That is why the transformation process must move swiftly. Strike while the iron is hot may be a very old and over used cliché, but never in the history of the Army has it ever been more reflective of a situation than what the Army is facing today.

QUADRENNIAL DEFENSE REVIEW (QDR)

The QDR is a principal DOD document, which lays out department strategy and direction for the next four years. In it are the macro guidelines and plans for how the department intends to conduct business and what changes in direction are projected for the next four-year cycle. This is the first QDR to mention transformation as the current Army Transformation started only three years ago, one year after the previous QDR was published. This QDR was published only nineteen days after the September 11 tragedy yet it contains the key ingredients necessary to accommodate the changed world DOD now must face. This was not all that surprising since the hand picked military department secretaries had been spending most of their time writing this document.¹³ From an IT perspective it is significant to note that this QDR significantly increases the importance of information as a technology and elevates it to a key role in every aspect of the DOD Transformation. This is substantiated in the QDR text on numerous occasions such as the following:

"Conducting Information Operations" is one of the four key military capabilities listed in the 2001 QDR (the other three are: "Conducting anti-access efforts," "Defending US and allied territories," and "Protecting US assets in Space."¹⁴

A second example of the elevated IT importance in the QDR has to do with the Information Operations (IO) as a key strategy.

"Space and information operations have become the backbone of networked, highly distributed commercial civilian and military capabilities. This opens up the possibility that space control...will become a key objective in future military competition. Similarly, states will likely develop offensive information operations and be compelled to devote resources to protecting critical information infrastructure from disruption, either physically or through cyberspace."¹⁵

The terms information operations and new information technologies are spread throughout the QDR Report. In terms of capabilities the term IO is the driver not IT as IO in the Military Information Environment (MIE) encompasses IT as one of its components. IO is defined as "continuous military operations within the MIE that enable,

enhance and protect the friendly force's ability to collect, process and act on information to achieve an advantage across the full range of military operations. IO includes interacting with the global information environment...."¹⁶ This is pretty broad both in peace and war, i.e. across the spectrum of conflict. The MIE is that portion of the Global Information Environment that consists of information, Information Technology (IT), information resources, information systems (INFOSYS) and organizations (friendly and adversary, military and non-military) that support, enable or significantly influence military operations. IO is comprised of three interrelated components, which are Operations, Relevant Information and Intelligence (RII), and INFOSYS. The 2001 QDR elevates Information Operations to a much higher level than the previous QDR. As the strategy moves from Shape, Respond, and Prepare to Assure, Dissuade, Deter, and Defeat, DOD realizes that greater emphasis must be placed on Information Operations as a means to accomplish these tasks. In so doing, we see that the increasing dependence being placed on this medium will demand greater protection for the infrastructure that drives it and greater sophistication in its functional capabilities. Also recognized is the high cost of developing and protecting these sophisticated systems, which resulted in the call to "Modernize DOD Business Processes and Infrastructure."¹⁷ Today's technology makes the accurate, timely flow of information possible. Pushing this information down will enable decision-making at the right level and will, in turn, support the flattening and streamlining of the organization. DOD must keep its information, communications, and other management on par with the best, proven technologies available. "Given the availability of advanced technology and systems to potential adversaries, dissuasion will also require the United States to experiment with revolutionary operational concepts, capabilities, and organizational arrangements and to encourage the development of a culture within the military that embraces innovation and risk-taking."¹⁸

Finally, the defense strategy calls for the transformation of the U.S. military and Defense establishment over time. "The Department's leadership recognizes that continuing business as usual within the Department is not a viable option given the new strategic era and the internal and external challenges facing the U.S. military. Without change the current defense program will only become more expensive to maintain over time. Without transformation, the U.S. Military will not be prepared to meet emerging challenges."¹⁹

Secretary of Defense Rumsfeld recently said that the success of the transformation could rest in the next 30 generals he selects to run the key positions in the military services. He made good on that statement by selecting what some might call controversial choices for many top military jobs.²⁰ What ties these selections to the transformation process is his reason for the controversial choices. He said he was looking for people who can think outside the box and

look for new ways of doing business in a rapid manner.²¹ That statement tells everyone that transformation is important and that those who are involved should support it.

SEPTEMBER 11, 2001

If September 11, 2001 has done anything with regard to the enhancement of the transformation processes going on in the military services today, it is to unify the resolve of the people of the United States to be receptive to doing what is necessary to get the military better prepared to most efficiently fight the new priorities of today's world. Homeland Defense is something America never had to consider until now. Airport security is another necessary but added expense. Border security and immigration and passport monitoring will be next followed by many other security protection enhancements never before considered because America thought it was safe from these types of attack. Transformation will be expensive. But if the American public sees a direct benefit for the added cost in terms of their personal security, they will be more receptive as long as the changes made are sensible and as efficient as possible.

THE PLAN

The Army had anticipated the increased IO emphasis and was already moving out on transforming prior to September 11. On August 8, 2001 the Secretary of the Army issued Army Knowledge Management Guidance Memorandum Number 1, which contained five goals that essentially called for an Army-wide cultural change to a knowledge-based organization that integrates best business practices to improve performance. The goal is to manage the infrastructure as a single enterprise operating from one Army-wide Enterprise Portal while harnessing the human capital needed to sustain the knowledge organization.²² "Army Knowledge Management (AKM) is the Army strategy to transform itself into a network-centric, knowledge-based force... AKM is intended to improve decision dominance by our war fighters and business stewards in the battle space, in our organizations, and in our mission processes."²³ The new organizational structure calls for sweeping changes.

The Army has not only issued implementing instructions to AKM Guidance Memorandum Number 1, but in many cases, it is already acting on much of the guidance. On 18 September 2001 the Army Chief Information Officer, LTG Peter Cuvillo, issued detailed implementing instructions to the Army announcing specific restrictions and responsibilities for all Major Army Commands.²⁴ For instance, The Army Knowledge Office (AKO) has consolidated and/or issued more than 850,000 e-mail accounts Army-wide since August.²⁵ This is the first step in consolidating all e-mail for the entire Army into one system.²⁶ Beginning with the second

quarter FY02, all IT infrastructure dollars will be centralized much the same way they were back in the days of Information Systems Command.²⁷ The entire system is headed toward a single managing agency for Army Information Operations. On December 6, 2001 the Vice Chief of Staff received an update briefing on Army Knowledge Management outlining the progress made thus far in this dynamic transformation. Detailed implementing instructions are being developed to consolidate all e-mail file servers in the Army into one or very few server farms. These farms will utilize large-scale processors/servers that are as large or larger than the computers currently in use at the six DOD Regional Computer Centers.²⁸

On March 16, 2002 U.S. Army Signal Command posted a draft Network Operations Concept of Operations for comment by the Army staff and all interested parties. This document outlines the new roles and responsibilities of the Network Enterprise Technology Command (NETCOM), a newly established Army Staff Field Operating Agency (FOA) under the Army CIO/G6, which will operate and manage the Army Enterprise Infostructure (AEI). NETCOM will have technical command, control and configuration management authority for the Army's critical networks and systems, and will have operational review/coordination authority for any standards, system, architecture, design, or device that impacts the AEI. While the AEI will be centrally managed, operations and maintenance can be delegated to other elements consistent with and under the review of NETCOM.²⁹

The current Army operating environment consists of a variety of geographically dispersed small, medium, and large installations and user sites (e.g., Reserve Component Centers, Armories, and Recruiting stations), in the Continental United States (CONUS) and outside the Continental United States (OCONUS). Small installations are characterized by having less than 5,000 user workstations, medium installations with 5,000 – 15,000 workstations and large installations having excess of 15,000 workstations. Additionally, on large installations, 400 or more e-mail, web, file, print, application, and other servers may be in operation. Medium installations may operate 200 or more servers, and small installations and sites, a lesser number. These installations host several IT facilities providing support to not only Army users but also to other Service/Agency tenants. In addition, the Army has many mobile users that will need access to the infostructure from outside the enclave. Thus, multiple separate communities of interest with varied IT requirements are found on most Army installations. Furthermore, the Operations and Management (O&M) of the IT systems at these locations differ from installation to installation. In some installations, O&M is performed by Army assets (military and civilian); in others a mix of Army and contractor support. Large headquarters complexes exist, such as Department of the Army headquarters in the Pentagon. There are several other large

commands located around the world in remote locations, such as the Army Corps of Engineers, Army Recruiting Command and Medical Command. Other organizations have activities and isolated users located in other government and commercial leased facilities throughout CONUS and in some cases, OCONUS. These many disparate operations will be transitioned to consolidated operations and management under NETCOM so as to provide efficiencies of operation and consistent service levels. Service Level Agreements (SLA) will manage user expectations for support and set standards to measure NETCOM performance.³⁰

ARMY KNOWLEDGE MANAGEMENT (AKM)

Some overall strategy would be necessary to consolidate all of the disparate pieces together into one interdependent system and serve as a method to migrate all systems and platforms to the desired end state. Army Knowledge Management is an ongoing project that was struggling for its existence that now takes center stage in light of the IT transformation emphasis posed by DOD senior leadership.

"Army Knowledge Management (AKM) is a comprehensive strategy to transform the Army into a network-centric, knowledge-based force. It consists of a robust set of goals and objectives that, once achieved, will improve decision dominance by tactical commanders and business stewards. The goals and objectives concentrate on managing the information technology infrastructure as an enterprise in line with the Global Information Grid, with a view toward reducing the footprint and creating ubiquitous access, through Army Knowledge Online as the enterprise portal, to knowledge, systems, and services. The use of best business and governance practices and the emphasis on innovative human capital strategies are key goals of AKM. Army Knowledge Management is a strategic transformer for the Army and is a key component of Army Transformation."³¹

Secretary of the Army White and Army Chief of Staff GEN Shinseki reinforced AKM strategic importance in the Forward of the AKM Strategic Plan.

"Our goal is decision superiority in the battlespace, in our organizations, and in our mission processes. To achieve this goal, our Army intellectual capital (individual, teams, organizations, systems, collaborative insights and experiences), infostructure capabilities, and governance structures must be optimized for effective decisions. This plan recognizes that becoming a knowledge-based organization involves more than just technologies. It requires deep cultural shifts... from traditional practices to collaboration, teamwork, and innovation; from information hoarding to knowledge sharing; from stovepipe systems and processes to enterprise ones; and from traditional skills to Internet-Age competencies."³²

The AKM goals can be summarized as follows:

- Adopt governance and cultural changes to become a knowledge-based organization.
- Integrate knowledge management concepts and best business practices into Army processes to improve performance.
- Manage the infostructure as an enterprise to enhance capabilities and efficiencies.
- Scale Army Knowledge Online as the Enterprise Portal to provide universal, secure access for the entire Army.
- Harness human capital for the knowledge organization.

The Army Enterprise Infostructure Transformation (AEIT) is the ongoing AKM Goal 3 effort to converge the disparate Sustaining Base and Tactical Information Technology environments that currently exist in the Active Army, the National Guard and the Army Reserve, into a single Army Enterprise while leveraging the unique capabilities of each. The AEIT will provide a seamless network throughout the Army, enabling the transformation of the Army into a knowledge-based, network centric force.³³

The consolidation of dollars, infrastructure, and user e-mail accounts are all directed toward standardization, streamlining, saving dollars and supplying greater power projection capabilities for IO to support the new DOD mission strategy. Since future adversaries are unknown and their locations undetermined, IO must be flexible, simple, easily transportable, immediately available and always operational. Transporting electrons instead of heavy computer hardware and software to the hotspots of the world will be critical to the success of the new DOD posture.

THE EFFECT

It appears that the Army is on target with the IO strategies outlined in the 2001 QDR. In fact, the Army may be ahead of the sister services in many respects and probably was the prime contributor to the IO approach taken in the QDR. A tremendous amount of planning and senior level preparation has already taken place, which shows how the Army is proactively poised to complying with QDR guidance. Because the AKM/NETCOM changes are in their early stages, most IT officials at the levels below the Army staff do not know the full significance of the changes about to be implemented. The Army IT community has never seen a change of this magnitude since its inception. The whole IT procedure will be changing. Budgets will be centralized as well as the authority to add new hardware or systems. The chain-of-command will be different with the DOIM being removed from local command authority. Even the location of the e-mail servers will be new.³⁴

Though the change is a much-needed one, and will take place over time, it will be met with resistance and will cause some disruption in normal operations. New lines of communication must be established. New ways of doing business must be learned. Politics will play a larger role since coordination and negotiation with people outside of the local organization could be key to achieving the desired outcome. Though not obvious in the early stages, in the long run the system should be much simpler because of standard communications and hardware, more reliable because of redundant back-up systems and greater control of the communications equipment.

THE OBJECTION

Even though there is wide spread support for the Army to implement major transformational changes in this area, it is not proceeding without major obstacles and some disgruntlement on the part of all Army commands. Protection of command areas of responsibility and normal resistance to major change are traditional reactions for middle and upper level commanders and are hard for them to modify. Command prerogative and responsibility make a commander completely responsible for everything the organization does or does not do. When parts of that organization are removed from direct command control, commanders are wary and believe they are being hampered in carrying out their responsibility. Previous history as outlined above has helped to set the stage for much of the current resistance to the transformation processes now under way. Commanders remember the difficulties of the past and transpose them on to the future as they try to predict future outcome. The Army Signal Command has been internally realigned to look like NETCOM. A provisional Table of Distribution and Allowance has been approved. The only remaining official act is the signing of the General Order which is expected any day. NETCOM works for the Army Chief Information Officer (CIO). The Directors of Information Management (DOIM) on most installations will now be a part of the Garrison staff reporting to the Regional Director who reports to the Assistant Chief of Staff for Installation Management (ACSIM).³⁵

To some this means losing control and authority. To others it is taking away something that was theirs and giving it to someone else to control, which reflects that the original owner did not manage it properly. That is not the case but it is hard to convince the affected parties. The immediate thought at the local level will be that the IT world is back where it started twenty years ago. The Commanders will have no control over what IT managers do or when they do it.

Even with the NETCOM stand up the objections could still manifest themselves in many ways depending on how open the command is to gathering information from all stakeholders on

what needs to be standardized, eliminated or realigned before the final decisions are made. If the Army Signal Command and Army CIO senior staff view the NETCOM realignment as an internal problem for them to solve among themselves then the transformation is doomed to failure because it will not address the problems of the customer base. The commander's original fears and suspicions will not be addressed. They will have no confidence in the change and history will, once again, repeat itself. Renaming the organization does not correct the problems.

This will be a major problem that can only be overcome by communication, training, education, persistence, senior level support, and buy-in. Had it not been for the September 11, 2001 tragedy, the problem would have been even more difficult to solve. Now, with an urgent need to see things differently, change is not as uncomfortable since everyone around us seems to be doing it. We must take advantage of all the forces that are at hand. Capitalize on what is different about the present set of circumstances and use that to begin the change process.

THE FUTURE

All of these changes in the Army beg the following question. If the consolidation and standardization moves undertaken by the Army make sense, why wouldn't consolidating all Information Operations for all DOD organizations into one system make even better sense? The trend seems to be toward a joint, more unified approach to war fighting. The concept of interjecting sound business practices in the war fighting strategy where appropriate also makes good sense. As each branch of service applies these factors to their own policies and practices, it is possible to see the thought process shift to several questions. Why do the Army and Navy each have an Air Force? Why does the Army have a Navy? Why do the Army and Marine Corps have similar ground forces? Why do all branches have a space command and an information systems command? As the major realignments underway at the senior levels of the Army, Air Force, and the Navy run to completion it is inevitable that the logic of continuing the transformation to eliminate the redundancies across the services becomes the next logical step. The key to simplifying the ultimate transformation across all branches of the military is the improvement, implementation and operation of the Global Information Grid (GIG). The evolution of IT will increasingly permit the integration of traditional forms of information operations with sophisticated all-source intelligence, surveillance, and reconnaissance in a fully synchronized information campaign. It would follow that the military service having the best capability for capturing certain types of information would be responsible for providing it to the Grid. The Grid will be the globally interconnected set of information capabilities, associated processes and

people to manage and provide information on demand to the warfighters, policy makers, and support personnel in all services. This means that the problem of passing real time data to the person needing it to make the best tactical decision possible is solved. If all parties have all available information needed to make the best decision possible in the required time frame, the service with the best ability to carry out the mission should have the responsibility for the execution. When all military information flow is secure, accurate, timely, and reliable and passes freely across all services, the need for redundant functions in the military services becomes a moot point. This is an ultimate long-range objective. There would be major obstacles to overcome in achieving this goal that would place it in the 2030 and later glide path for completion.

CONCLUSION

The world has changed. National priorities have changed. Enemies of the future most likely will not be the enemies of the past. The approach to war will be completely new. The Army is a very large, traditional organization that has needed a major transformation to bring itself in line with current needs and thinking. Information technology has a key role to play in making the Army transformation successful. History has shown that the IT management sins of the past will add some difficulty to the transition burden. It is not that major changes have not been attempted previously. They most definitely have. Unfortunately, each time some key ingredient was missing or withdrawn, priorities shifted or support slackened over time. Today, more than ever before, the need to make this transformation a successful reality is more critical than at any other time in our past. Fortunately, or perhaps even miraculously, all of the critical ingredients for success are present and actively working towards that goal. There is a plan, an organization, senior DOD and Army leadership and management support, public support, and financial backing to bring this to reality.

These factors alone will not guarantee success. Management must act quickly, responsibly, and objectively for the good of the Army as a whole and not for the short-sided objectives of individual areas of responsibility. The key ingredients that are in place now are time sensitive. To get the maximum effect the plan must be implemented immediately and the people trained to operate under the new guidelines. Middle management must be educated to understand, accept and support the coming changes. They must be taught that change will be the only constant in the future. Adjustments will be constant and continuous. There is no final objective. The Army cannot wait for the perfect answer before transforming. Corrections along the way are the acceptable method of change. If these tasks are not accomplished while the

critical ingredients are in place, momentum will be lost and the transformation will fail once again, as it has in all previous attempts.

Word count = 6054

ENDNOTES

¹ Department of the Army, United States Army Information Systems Command : History (Fort Huachuca, AZ.:U.S. Department of the Army, FY 1992),

² Personal notes and conversations with other DOIM's, installation commanders, and other installation personnel at conferences, conventions, and committee meetings over many years.

³ My personal experiences of eleven years as a Director of Information Management (DOIM) at three Army installations.

⁴ Personal notes and conversations with other DOIM's, installation commanders, and other installation personnel at conferences, conventions, and committee meetings over many years.

⁵ Personal experience from over 32 years of service as an Army IT officer and civilian employee having served in various positions at eight different locations nationwide.

⁶ Department of the Army, United States Army Information Systems Command Annual Review (Fort Huachuca, AZ.:U.S. Department of the Army, FY 1992), Appendix A.

⁷ Personal experience from over 32 years of service as an Army IT officer and civilian employee having served in various positions at eight different locations nationwide.

⁸ Ideas in this paragraph are based on remarks made by a speaker participating in the U.S. Army War College Commandant's Lecture Series.

⁹ Paul Wolfowitz, Deputy Secretary of Defense, DOD News Briefing on Management and the Service Secretaries, (Washington, D.C.), 18 June 2001. Available from <http://www.defenselink.mil/news.html>, Internet: Accessed 6 March 2002.

¹⁰ Information taken from the biographies of the Deputy Secretary of Defense, Paul Wolfowitz, Secretary of the Army, Thomas E. White, Secretary of the Navy, Gordon England, and Secretary of the Air Force, Dr. James G. Roche. Available from <http://www.defenselink.mil/bios.html>, Accessed 6 March 2002.

¹¹ Information taken from the biography of Secretary of Defense, Donald H. Rumsfeld. Available from <http://www.defenselink.mil/bios.html>, Accessed 6 March 2002.

¹² The ideas in this paragraph are based on remarks made by Secretary of Defense Donald Rumsfeld to the National Defense University. Topic: Defense Transformation, Ft. McNair, (Washington D.C.), 31 January 2002.

¹³ Ibid

¹⁴ Department of Defense, Quadrennial Defense Review Report (Washington D.C.:U.S. Department of Defense, 30 September 2001),7.

¹⁵ QDR 51-56.

¹⁶ Department of the Army, Information Operations, Army Field Manual 100-6 (Washington, D.C.: U.S. Department of the Army, August 1996), 1-4.

¹⁷ QDR, 15.

¹⁸ QDR, 12.

¹⁹ QDR, 16.

²⁰ Thomas E. Ricks, "Bush Backs Overhaul of Military's Top Ranks" Washington Post, 11 April 2002, sec. A., p.1.

²¹ Ibid

²² Miriam F. Browning, "Army Knowledge Management (AKM) Brief for General John G. Coburn, AMC," briefing slides, Washington D.C., 21 August 2001.

²³ Secretary of the Army Thomas E. White, "Army Knowledge Management Guidance Memorandum Number 1," memorandum for see distribution, Washington D.C., 08 August 2001.

²⁴ Army CIO, LTG Peter Cuvillo, "Army Knowledge Management Implementing Instructions Number 1," memorandum for see distribution, Washington, D.C., 08 September 2001.

²⁵ Wade, Roderick K., Program Manager (PM) Army Knowledge Management, Army Knowledge Online Office, interview by author, 11 February 2002, Ft. Belvoir, VA

²⁶ Catherine Michaliga, "Army Knowledge Management (AKM), Update Briefing for LTG Cuvillo" briefing slides, Washington, D.C., 27 September 2001.

²⁷ Ibid.

²⁸ Roe, John C., Chief, Strategic Planning, Office of the CIO, U.S. Army Materiel Command, interview by author, 05 October 2001, and 11 February 2002, Alexandria, VA.

²⁹ Information in this paragraph is based on information contained in the U.S. Army Signal Command Network Enterprise Technology Command (NETOPS) Concept of Operations (CONOPS) Version 1.1 Draft: 16 March 2002.

³⁰ Ibid

³¹ Army Knowledge Management, A Strategic Plan for an Agile Force, Version 2.1, U.S. Army CIO Office 8 August 2001.

³² Secretary of the Army Thomas E. White & Army Chief of Staff Eric K. Shinseki, Army Knowledge Management Strategic Plan, Forward, Washington, D.C., 21 October 2001.

³³ Cuiello, Peter M, U.S. Army Chief Information Officer. "Army Knowledge Management Implementing Instructions Number 1." Memorandum for See Distribution. Washington D.C., 18 September 2001.

³⁴ Information in this paragraph is based on information contained in the U.S. Army Signal Command Network Enterprise Technology Command (NETOPS) Concept of Operations (CONOPS) Version 1.1 Draft: 16 March 2002.

³⁵ Gullo Louis, LTC, Series of e-mail traffic between Information Systems Command and Army Material Command outlining the details of the Army Signal Command realignment, (Washington D.C.) 1-26 April 2002.

BIBLIOGRAPHY

- Browning, Miriam F., "Army Knowledge Management (AKM) Brief for General John G. Coburn, AMC," briefing slides. Washington D.C: U.S. Army Materiel Command, 21 August 2001.
- Buckner, James, Chief Information Officer for U.S. Army Materiel Command, interview by author, 05 October 2001, Alexandria, VA.
- Cuviello, Peter M, U.S. Army Chief Information Officer, "Army CIO Executive Board Meeting Briefing," briefing slides, Washington D.C., 30 October 2001.
- Cuviello, Peter M, U.S. Army Chief Information Officer. "Army Knowledge Management Implementing Instructions Number 1." Memorandum for See Distribution. Washington D.C., 18 September 2001.
- Garamone, Jim, "Flexibility, Adaptability at the Heart of Military Transformation" American Forces Press Service, 31 January 2002. Available from http://www.defenselink.mil/news/jan2002/n01312002_200201313.html . Accessed 1 February 2002.
- Hoffman, Rich, "The IT Road Ahead Windows 2K and Exchange 2K AKM Baseline Survey" briefing slides, Washington D.C., 24 August 2001.
- Michaliga, Catherine, "Army Knowledge Management (AKM) Update Briefing for LTG Cuviello," briefing slides, Washington D.C., 27 September 2001.
- Roche, James G, "Transforming the Air Force" Joint Forces Quarterly, Autumn-Winter 01-02 issue, pp 9-14.
- Roe, John C., Chief, Strategic Planning, Office of the CIO, U.S. Army Materiel Command, interview by author, 05 October 2001, and 11 February 2002, Alexandria, VA.
- U.S. Department of the Army. Information Operations. Army Field Manual 100-6. Washington D.C.: U.S. Department of the Army, 21 October 2000.
- U.S. Department of the Army. Army Signal Command. Draft NETOPS CONOPS version 1.1. Washington D.C., 16 March 2002.
- U.S. Department of Defense. Quadrennial Defense Review Report. Washington D.C.: U.S. Department of Defense, 30 September 2001.
- Wade, Roderick K., Program Manager (PM) Army Knowledge Management, Army Knowledge Online Office, interview by author, 11 February 2002, Ft. Belvoir, VA.
- White, Thomas E, Secretary of the Army, "Army Knowledge Management Guidance Memorandum Number 1." Memorandum for See Distribution. Washington D.C., 08 August 2001.
- Paul Wolfowitz, Deputy Secretary of Defense, "DOD News Briefing on Management and the Service Secretaries", (Washington, D.C.), 18 June 2001. Available from <http://www.defenselink.mil/news.html>, Internet: Accessed 6 March 2002.